Cisco Systems

ciscopress.com

VPN 故障诊断与排除

Troubleshooting Virtual Private Networks

Master advanced troubleshooting techniques for IPSec, MPLS Layer-3, MPLS Layer-2 (AToM), L2TPv3, L2TPv2, PPTP, and L2F VPNs

[美] Mark Lewis, CCIE #6280 著

袁国忠 等 译

人民邮电出版社
POSTS & TELECOM PRESS

VPN 故障诊断与排除

[美] Mark Lewis, CCIE #6280 著

袁国忠 等 译

人 民 邮 电 出 版 社

图书在版编目（CIP）数据

VPN 故障诊断与排除 /（美）刘易斯（Lewis, M.）著；袁国忠等译.
—北京：人民邮电出版社，2006.2

ISBN 7-115-14314-5

Ⅰ. V... Ⅱ. ①刘... ②袁... Ⅲ. ①虚拟网络－故障诊断 ②虚拟网络－故障修复
Ⅳ. TP393.01

中国版本图书馆 CIP 数据核字（2006）第 003737 号

版 权 声 明

VPN 故障诊断与排除

◆ 著 [美] Mark Lewis, CCIE # 6280
译 袁国忠 等
责任编辑 李 际

◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号
邮编 100061 电子函件 315@ptpress.com.cn
网址 http://www.ptpress.com.cn
北京顺义振华印刷厂印刷
新华书店总店北京发行所经销

◆ 开本：787 × 1092 1/16
印张：37.5
字数：914 千字 2006 年 2 月第 1 版
印数：1－3 500 册 2006 年 2 月北京第 1 次印刷

著作权合同登记号 图字：01-2006-0301 号

ISBN 7-115-14314-5/TP • 5172

定价：78.00 元

读者服务热线：(010)67132705 印装质量热线：(010)67129223

内容提要

本书不但介绍了排除 VPN 故障的命令和技巧，而且包含正确地解释故障排除命令输出所需的详细协议信息。全书包含相互独立的 8 章，它们是为快速、简明地排除故障而设计的，提供了有关解决各种常见和不那么常见的 IPSec VPN、MPLS 第 3 层 VPN、基于 AToM（Any Transport over MPLS）的第 2 层 VPN、基于 L2TPv3 的第 2 层 VPN、L2TPv2 VPN、PPTP VPN 和 L2F VPN 故障的详细信息。本书不但介绍了如何解决问题，还介绍了如何使用专家级 VPN 配置指南和优化技巧来避免问题。

每章都包含针对不同 VPN 技术的端到端的循序渐进故障排除方法。深入的技术讨论和配置简介让读者熟悉 VPN 技术，为故障排除做准备。为帮助读者获得所需的解决方案，每章都有故障排除流程图，提供了快速获取问题解决方案的路线图。在每章的末尾都有案例研究和复习题，前者提供了复杂或不常见问题的解决方案，后者可帮助读者检查对知识的掌握程度。另外，还提供了故障排除实验，帮助读者巩固在本书中学到的技能。

本书适合那些负责管理和部署 Cisco IOS VPN 的网络工程师、管理员和设计师阅读，也可供备考服务提供商和安全（Service Provider 和 Security）考试的 CCIE 考生参考。

关于作者

Mark Levis（CCIE No. 6280）是 MJL Network Solution（www.mjlnet.com）公司的技术总监，这是一家领先的网络互连解决方案提供商，致力于帮助服务和企业提供商客户实现最前沿的技术、部署安全解决方案和优化网络，并提供高级培训服务。Mark 擅长 VPN 技术，有多年设计、实现和排除 IP 网络故障的经验。他还是 MCSE + I 和 Cisco Systems 认证的讲师。Mark 的电子邮件地址为 mark@mjlnet.com。

关于技术审稿人

Henry Benjamin（CCIE No. 4695）拥有 3 个 CCIE 认证（路由和交换、ISP 拨号以及通信和服务）。他有十多年 Cisco 网络从业经验，现就职于 Cisco 的内部 IT 部，致力于帮助设计和实现遍及澳大利亚和亚洲的网络。Henry 是 CCIE 全球小组的重要成员，负责为 CCIE 考试编写新的实验题。Henry 是澳大利亚一家大型网络安全公司的独立咨询师。

Robert Brown（CCIE No. 7309）是 Cisco 输出解释器（Output Interpreter）的开发人员兼技术带头人。Cisco 输出解释器是一种功能强大的在线故障排除工具，提供有关 Catalyst、IOS 和 PIX 设备的故障排除建议。他作为加密电子技术人员和电话系统专家在美国空军工作了 10 年。加入 Cisco Systems 之前，他曾在 TRW、Litton PRC 和 International Network Services 就职。

Nathan Lohr（CISSP、CCSP 和 CCNA）是 TRL Secure Solutions 的总裁，这是一家位于弗吉尼亚的小型公司，提供国内和国际安全咨询和培训服务。在过去的 15 年中，他设计、测试和验证过 VPN、防火墙、入侵检测和事故应对解决方案，还帮助客户确保其遵循了 HIPAA 和 DCID 要求。

Andrew Makin 是位于英国的 Cisco 金牌合作伙伴 Energis 的一名网络咨询人员，当前拥有 CCNP、CCDP 和 CSS-1 证书。他为客户设计 WAN 解决方案，涉及跨越 Internet 和 Energis 的提供商网络的 IP 和安全 VPN 技术。

Ivan Pepelnjak（CCIE No. 1354）有十多年设计、安装、维护和运营大型服务提供商和企业 WAN 和 LAN 网络的经验，现为 NIL Data Communications 的首席技术顾问。他是 NIL 的服务提供商技术学院项目的设计师、Cisco Systems 服务提供商课程的设计师之一以及多门服务提供商课程的首席开发人员，这些课程涵盖了 MPLS、边界网关协议（BGP）和 IP 服务质量。在欧洲，Ivan 是 Cisco 路由选择技术方面的权威人士之一。

Tim Sammut（CCIE No. 6642）是 Northrop Grumman Information Technology 的一位资深网络咨询人员，在涉及从 LAN 交换、安全和 SAN 集成等技术的项目中扮演过重要的角色，帮助过众多的组织（用户数量从 100 到 130 000）充分利用其网络投资。Tim 还拥有 CISSP、CCIE 安全以及 CCIE 通信和服务等认证。

Wen Zhang 从 1997 年 6 月起便是 Cisco 技术支持中心（TAC）负责安全和 VPN 技术的成员，从 2000 年 8 月起是 TAC 扩大小组的成员。Wen 经常给 Cisco 开放论坛撰稿，拥有 Clemson 大学的学士和硕士学位。

前　言

各种形式的虚拟专网（VPN）在全球越来越普及。对服务提供商和企业来说，VPN 提供了一种通过广域网支持新服务和应用，同时极大地节省费用的方法。

VPN 很复杂，因此出现故障时很难排除。如何办呢？一种选择是同 Cisco TAC 联系；另一种选择是购买本书，卷起您的袖子，自己动手排除故障。本书涵盖了尽可能多的信息，有了它读者将能够很好地解决遇到的问题。如果读者的组织正考虑部署或优化 VPN，并希望避免发生本书描述的问题和其他问题，请访问作者的公司网站（www.mjlnet.com）或与作者本人联系，知识渊博的作者同事或作者本人将及时赶到现场，帮助确保这一过程顺利地完成，当然，我们的服务是收费的！另外，如果读者的组织要通过高级培训提高员工的工作效率和专业知识水平，也可访问本公司的网站。

本书引用了大量的 RFC 和 Internet 草案，其中的很多都可在 IETF 网站（www.ietf.org）中找到。然而，Internet 草案会过期，因此另一种找到它们的方法是使用诸如 www.watersprings.org 等档案网站。

本书的目的

在作者设计、实现和排除 VPN 故障的工作中，发现目前找不到这样的资料：不但介绍排除 VPN 故障的命令和技巧，而且包含正确地解释故障排除命令输出所需的详细协议信息。本书旨在提供这样的信息源，希望它能帮助读者在排除 VPN 故障时节省大量的时间和精力。

针对的读者

本书涵盖了各种 VPN 技术，包括 IPSec、MPLS、L2TPv3、L2TPv2、PPTP 和 L2F。适合那些从事 VPN 日常支持工作或部署 VPN 的支持工程师和设计师阅读。

由于涵盖的范围非常广，每章不但介绍了故障排除，还包括技术概述和配置指南，因此本书可能对备考服务提供商和安全（Service Provider and Security）考试的 CCIE 考生有极大的帮助。

本书的内容结构

可以 3 种不同的方式阅读本书。首先，可以从头到尾地阅读，如果读者想大概地了解 VPN 技术和提高网络互连技能，可采用这种阅读方式。

第二种方式是，在问题出现前，阅读与您的网络使用的 VPN 技术相关的章节。这不失为一个好主意，有备无患嘛！

最后，可以在发生问题时阅读相关的章节。每章都以尽可能方便阅读的方式组织的。

另外，还提供了大量的故障排除实验，帮助读者提高和磨砺 VPN 故障排除技能。在 Cisco Press 网站（www.ciscopress.com/1587051044）上，包含 L2F、L2TPv2、MPLS 第 3 层 VPN 和 IPSec 故障排除实验。没有提供 PPTP 故障排除实验，因为 Cisco IOS 路由器只支持自发隧道模式，且可能的客户操作系统非常多；也没有提供 L2TPv3 和 Any Transport over MPLS（AToM）故障排除实验，因为编写本书时，这些技术要求的最低端平台为 Cisco 7200——作者无法想象，很多读者会有那么幸运，在其实验室中有 7200 系列路由器。

如果 Cisco 在更低端的平台中添加了对 L2TPv3 和 AToM 的支持，作者可能开发一些针对这些技术的实验。在这种情况下，请读者访问 Cisco Press 网站。读者还可能找到一两个针对本书讨论的其他技术的实验。

本书包括如下章节：

第 1 章“基本的故障排除方法”：简要地介绍了一种基本的端到端故障排除方法，它非常适合用于 VPN；还讨论了用于排除 VPN 故障的工具和技巧。

第 2 章“第 2 层转发协议 VPN 故障排除”：L2F 是最早使用的虚拟专用拨号网络技术之一，本章讨论了这种技术及其配置，深入探讨了其故障排除技巧。

第 3 章“点到点隧道协议 VPN 故障排除”：本章讨论了 PPTP 协议及其配置，深入探讨了其故障排除技巧。

第 4 章“第 2 层隧道协议第 2 版 VPN 故障排除”：L2TP 是基于 L2F 和 PPTP 的，本章简要地介绍了 L2TP，讨论了其配置，深入探讨了 L2TPv2 故障排除技巧。

第 5 章“基于 L2TPv3 的 VPN 故障排除”：L2TPv3 是一种这样的技术：不但支持 PPP 的隧道化，还支持其他第 2 层协议（如以太网、HDLC 和帧中继）的隧道化。本章讨论了这种技术及其配置，深入探讨了其故障排除技巧。

第 6 章“多协议标签交换第 3 层 VPN 故障排除”：MPLS 第 3 层 VPN 是一种在服务提供商和企业中非常流行的技术。本章讨论了这种技术及其配置，深入探讨了其故障排除技巧。

第 7 章“基于 AToM 的 VPN 故障排除”：AToM 可用于通过 MPLS 主干传输诸如 HDLC、PPP、帧中继和以太网等第 2 层协议的数据报。本章讨论了这种技术及其配置，深入探讨了其故障排除技巧。

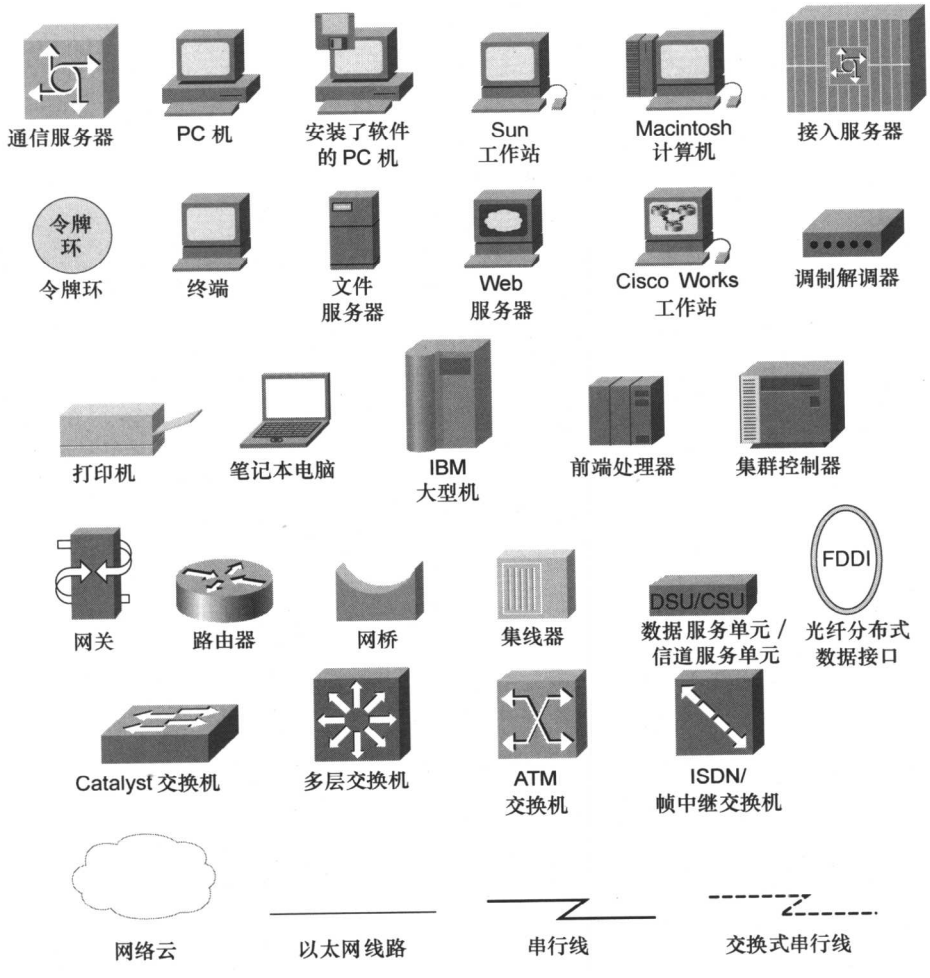
第 8 章“IPSec VPN 故障排除”：IPSec VPN 同样用于提供安全的场点到场点 VPN 或远程接入 VPN。本章讨论了 IPSec 技术及其配置，深入探讨了其故障排除技巧。

附录 A“复习题答案”：本附录包含每章末尾复习题的答案。

附录 B“实验说明和解决方案”：有关 L2F、L2TPv2、MPLS 第 3 层 VPN 和 IPSec 的章提供了故障排除实验，以帮助读者理解和巩固讨论的概念和技巧。本附录解释了如何从 Cisco Press 网站（www.cisco press.com/1587051044）将配置文件加载到实验路由器中，并提供了实验的解决方案。

本书使用的图标

本书使用如下图标来表示网络设备：



命令语法约定

本书在介绍命令语法时使用的约定与《IOS 命令参考手册》相同，这些约定如下：

- 需要逐字输入的命令和关键字用**粗体**表示。在配置范例和输出（而不是命令语法）中，需要用户手工输入的命令用粗体表示（如命令 **show**）。
- 用户必须提供实际值的参数用*斜体*表示。

- 互斥的元素用（|）隔开。
- 可选元素用[ ]括起。
- 必不可少的选项用{ }括起。
- 可选元素中必不可少的选项用[{ }]括起。

目　录